DEPARTMENT OF TECHNOLOGY & INFORMATION

DELIVERING TECHNOLOGY THAT INNOVATES

eSecurity News — Cyber SAFETY During the Holidays

DigiKnow
CYBER SECURITY DEPENDS ON YOU

Cyber Safety Depends On You

In today's digital world, online safety should be of paramount concern for individuals and organizations because the threats posed by cyber criminals can't be ignored. To counteract these threats, there are steps you can take to minimize the risks associated with doing business online, surfing the Internet, and/or sharing information on social media sites. (Simple Steps for Internet Safety)

- ☑ Keep a clean machine free from malware and infections by running only the most current version of applications and software.
- ☑ Use unique accounts and passwords for each account to help thwart cybercriminals.
- ☑ Use a password tracking tool to make it easier for you to manage passwords.
- ☑ Change your password or passphrase frequently.
- ☑ Disable Wi-Fi and Bluetooth when it is not in use so your movement cannot be tracked.
- ☑ Public Wi-Fi is not secure — do not use it for any transactions with a credit card or your personal data.
- ☑ Be an educated user and understand how to spot the most frequent types of threats, such as phishing attacks.

Questions or comments? Email us at eSecurity@state.de.us

Visit the DTI eSecurity website for previous issues of eSecurity Newsletters

Online Holiday Shopping

Anything connected to the Internet, including mobile devices like smartphones and tablets should be protected, especially during heavy use periods like the holidays. Scammers and cybercriminals target shoppers. Be on the alert for emails about problems with credit cards, your accounts or the status of any online orders.

For additional information, check the Federal Trade Commission's and USA.gov's resources for Online Shopping and watch the video.

Prepare, Prevent & Protect

Prepare: Be informed and have a plan for your online shopping excursions. Read reviews and evaluate positive and negative experiences of other shoppers. Read the return policy so you know what to expect if things don't go as planned. Use well known websites that you trust. Consider checking out as a guest rather than creating an account with the merchant.

Prevent Malicious Activity: Delete emails, social media posts and texts that contain links. Cybercriminals may be trying to steal your information or infect your devices. Follow the tips in the DigiKnow section of this newsletter.

Protect Personal Information and Money: Be alert to information being collected. Is it necessary? Is the site security enabled? Look for web addresses with *"https://"* indicating the extra measures taken to secure your information. Don't agree to let the merchant save your credit card details. Consider using a credit card that offers buyer protection allowing you to seek credit from the issuer if the product isn't delivered or was the incorrect item. Use a separate card for all your online shopping and set low credit limits. Always monitor your bank statements.

This newsletter is published by the Delaware Department of Technology and Information and sent to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links, or would like a printable copy (PDF), go to http://extranet.dti.state.de.us/information/dtie_information_eSecurity.shtml (links will only work if you are located in a state building or are using VPN to connect to the state network).